GMC INSTRUMENTS

DATA PROTECTION GUIDELINE

OF GMC-INSTRUMENTS GMBH

Table of Contents

1 Objective of this Data Protection Guideline

- In the context of its social responsibility, the GMC-Instruments GmbH (GMC-I Gruppe) undertakes to comply with international data protection and privacy regulations. This Data Protection Guideline is based on globally accepted basic principles of data protection. The protection of data privacy is a basis for trusting business relations and the reputation of the Group.

- This Data Protection Guideline creates one of the necessary framework conditions for the worldwide transfer of personal data between the companies of the GMC-I Group. It guarantees the appropriate level of data protection for domestic and cross-border data traffic required by the European General Data Protection Regulation (GDPR) and national laws, even in countries where there is no adequate level of data protection (third countries).

2 Definitions

- An adequate level of data protection in third countries is recognised by the EU Commission if the core of privacy, as it is understood unanimously in the EU member states, is essentially protected. In its decision, the EU Commission takes into account all circumstances that play a role in a data transfer or a category of data transfers. This includes the assessment of national laws as well as the applicable professional standards and security measures.

- Data are anonymised if a personal reference can no longer be established permanently and by anyone or if the personal reference could only be restored with unreasonably high expenditure of time, costs and labour.

- Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

- Sensitive data means data concerning racial and ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or the health or sexual life of the data subject. Under national law, further data categories may be classified as sensitive or the data categories may have different contents. In addition, data relating to criminal offences may often only be processed under special conditions laid down by national law.

- For the purposes of this Data Protection Guideline, data subject means any natural person about whom data are processed. In some countries, also legal persons may be data subjects.

- Data protection incidents are all events in which there are reasonable grounds to suspect that personal data were illegally spied on, collected, modified, copied, transmitted or used. This can refer to actions by third parties as well as employees.

- Third party means everyone outside the data subject and the body responsible for data processing.

- Within the EU, contract data processors or contract processors are no third parties in the sense of data protection law, as they are legally assigned to the controlling body.

- Third countries in the sense of this Data Protection Guideline are all countries outside the European Union/EEA. This does not apply to countries whose level of data protection has been recognised as adequate by the EU Commission.

- Consent is a voluntary, legally binding declaration of consent to data processing.

- Data protection officer (DPO): The company‘s data protection officer supports the company‘s self-monitoring („internal control“). The relevant legal regulations on designation as well as the rights and obligations of the DPO are described in Articles 37 to 39 GDPR and nationally (Germany) in Section 38 BDSG.

- The processing of personal data is necessary if the permissible purpose or the legitimate interest cannot be achieved without the respective personal data or only with unreasonable effort.

- The European Economic Area (EEA) is an economic area associated with the EU, to which Norway, Iceland and Liechtenstein belong.

- Personal data means any information relating to an identified or identifiable natural person (hereinafter “data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

- Transfer means any disclosure of protected data by the controlling body to third parties.

- Processing of personal data means any operation which is performed, whether or not by automated means, for the collection, recording, organisation, storage, alteration, retrieval, use, disclosure, transfer, dissemination or the combination and alignment of data. This also includes the disposal, deletion and blocking of data and data carriers

- Controlling body or controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

3 Scope of Application and Amendments of the Data Protection Guideline

- This Data Protection Guideline applies to all companies of the GMC-I Group.

- This Data Protection Guideline covers all processing operations of personal data. In countries where data of legal persons are protected in the same way as personal data, this Data Protection Guideline also applies in the same way to data of legal persons. Anonymised data, e.g., for statistical evaluations or investigations, are not subject to this Data Protection Guideline.

- The individual companies of the GMC-I Group are not entitled to make regulations deviating from this Data Protection Guideline, unless these have been released by the holding company of the GMC-I Group, GMC-Instruments GmbH (GMC-I), before they come into force.

4 Validity of National Law

- This Data Protection Guideline contains basic data protection principles without replacing existing national law. It supplements the respective national data protection legislation. The respective national law has precedence if it requires deviations from this Data Protection Guideline or makes more extensive requirements. The provisions of this Data Protection Guideline must also be observed if there is no corresponding national law. The reporting obligations for data processing under national law must be adhered to.

- Each company of the GMC-I Group is responsible for complying with this Data Protection Guideline and the legal obligations. If there is reason to believe that legal obligations conflict with the obligations under this Data Protection Guideline, the company concerned must immediately inform the GMC-I Group‘s management. In the event of a conflict between national legislation and this Data Protection Guideline, the GMC-I Group will work with the company concerned to find a practicable solution in line with the objectives of this Data Protection Guideline.

5 Principles Relating to Processing of Personal Data

5.1 Fairness and Lawfulness

- In the processing of personal data, the personal rights of the data subject must be protected. Personal data must be collected and processed lawfully and fairly.

5.2 Purpose Limitation

- The processing of personal data may only pursue the purposes defined before the collection of the data. Subsequent changes to the purposes are only possible to a limited extent and require justification.

5.3 Transparency

- The data subject must be informed about the handling of his or her data. In principle, personal data shall be collected right from the data subject. When collecting the data, the data subject must at least be able to recognise the following or be informed accordingly at the time of collection about:
  - The identity of the controlling body
  - The purpose of data processing
  - The contact details of the data protection officer
  - Third parties or categories of third parties to whom the data may be disclosed
  - The storage period or the criteria for erasure

- The right to lodge a complaint with a supervisory authority
- The right to information, correction, restriction, revocation
- The origin of the data (If the data were not collected from the data subject.)

5.4 Data Avoidance and Data Minimisation

- Prior to the processing of personal data, it must be checked whether and to what extent this is necessary in order to achieve the purpose intended by processing. If it is possible to achieve the purpose and the effort is proportionate to the intended purpose, anonymised or statistical data must be used. Personal data must not be stored in stock for potential future use unless required or permitted by national law.

5.5 Deletion

- Personal data that are no longer required after expiry of legal or business process-related retention periods must be deleted or destroyed, unless in individual cases there is an interest worthy of protection in storing them beyond this.

5.6 Factual Accuracy and Timeliness of Data

- Personal data must be correct, complete and - where required - up to date when stored. Appropriate measures shall be taken to ensure that inaccurate, incomplete or outdated data are deleted, corrected, supplemented or updated.

5.7 Confidentiality and Data Security

- Personal data are subject to data secrecy. They must be treated as confidential on a personal level and secured with suitable organisational and technical measures to prevent unauthorised access, illegal processing or disclosure, as well as accidental loss, modification or destruction.

6 Admissibility of Data Processing

- Collecting, processing and using personal data is admissible only under the following legal justifications for consent. Such legal justification for consent is also required if the purpose for the collection, processing and use of personal data is to be changed from its original purpose.

6.1 Customer and Partner Data

6.1.1 Data Processing for a Contractual Relationship

- Personal data of the prospective or actual customer or partner concerned may be processed to establish, execute and terminate a contract. This also includes advisory services for the partner under the contract if this is related to the contractual purpose. Prior to a contract – i.e., during the contract initiation phase – personal data may be processed to prepare bids or purchase orders or to fulfil other requests of the prospective customer that relate to contract conclusion. Prospective customers may be contacted during the contract preparation process using the data that they have provided. Any restrictions requested by the prospected customer must be complied with. For further advertising measures, the following requirements must be observed.

6.1.2 Data Processing for Advertising Purposes

- If the data subject contacts a GMC-I Group company to request information (e.g., request to receive information material about a product), data processing to meet this request is permitted.

- Customer loyalty or advertising measures are subject to further legal requirements. Personal data may be processed for advertising purposes or market and opinion research, provided that this is consistent with the purpose for which the data were originally collected. The data subject must be informed about the use of his/her data for advertising purposes. If data are collected exclusively for advertising purposes, their disclosure by the data subject is voluntary. The data subject shall be informed of the voluntariness of providing data for these purposes. When communicating with the data subject, consent shall be obtained from him/her to process the data for advertising purposes.

- If the data subject disagrees with the use of his or her data for advertising purposes, further use of his or her data for these purposes is not permitted and must be blocked accordingly. Any other existing restrictions in some countries regarding the use of data for advertising purposes must be observed.

6.1.3 Consent to Data Processing

- Data may be processed on the basis of the consent of the data subject. Before giving consent, the data subject must be informed in accordance with 5.3. of this Data Protection Guideline. For the purpose of documentation, the declaration of consent must always be obtained in writing or electronically. Under certain circumstances, e.g., in the case of telephone consultation, consent may also be given verbally. The granting of consent must be documented.

6.1.4 Data Processing Pursuant to Legal Authorisation

- The processing of personal data is also permissible if national legislation requires, presupposes or permits such processing. The type and extent of data processing must be necessary for the legally authorised data processing activity and must comply with the relevant statutory provisions.

6.1.5 Data Processing Pursuant to Legitimate Interest

- Personal data may also be processed if this is necessary for the realisation of a legitimate interest of the GMC-I Group. Legitimate interests are generally of a legal nature (e.g., collection of outstanding receivables) or commercial nature (e.g., avoiding breaches of contract). Personal data must not be processed on the basis of a legitimate interest if, in individual cases, there is evidence that the data subject's interests worthy of protection have precedence over the interest in the processing. The interests worthy of protection shall be examined for each processing. The justification for legitimate interests must be approved by the management of the Group.

6.1.6 Processing of Sensitive Data

- Sensitive personal data may only be processed if this is required by law or if the data subject has expressly consented to it. The processing of these data is also permissible if it is absolutely mandatory in order to assert, exercise or defend legal claims against the data subject. If the processing of sensitive data is planned, the Group's data protection officer must be informed in advance.

6.1.7 Automated Individual Decisions

- Automated processing of personal data, through which individual personal aspects (e.g., creditworthiness) are assessed, must not be the sole basis for decisions that have negative legal consequences or could significantly impair the data subject. The data subject must be informed of the fact and the result of an automated individual decision and given the opportunity to comment. To avoid wrong decisions, a control and a plausibility check by an employee must be guaranteed.

- Such automated processing activities must not be conducted in the GMC-I Group.

- Should this be necessary in individual cases, they must be approved by the management of GMC-Instruments GmbH prior to their introduction.

6.1.8 User Data and Internet

- If personal data are collected, processed and used on websites or in apps, the data subjects must be informed about this in privacy notices and, if applicable, cookie notices. The privacy notices and, if applicable, cookie notices must be integrated in such a way that they are easily recognisable, immediately accessible and constantly available to the data subjects.

- If user profiles are created (tracking) to evaluate the usage behaviour of websites and apps, the data subjects must always be informed of this in the privacy notices. Personal tracking may only be effected if it is permitted under national law or upon consent of the data subject. If the tracking is done under a pseudonym, the data subject should be given an opportunity to object in the privacy statement (opt-out).

- If a website or app has access to personal data in an area requiring registration, the identification and authentication of the data subjects must be designed in such a way that appropriate protection is achieved during access. If guidelines for identity and authentication management exist in individual companies, they must be designed accordingly and are binding.

6.2 Employee Data

6.2.1 Data Processing for the Employment Relationship

- In employment relationships, personal data may be processed if needed to establish, implement and terminate the employment contract. When initiating an employment relationship, the applicants' personal data may be processed. After rejection, the applicant's data must be deleted, taking into account the time limits for the retention period, unless the applicant has consented to further storage for a later selection process. Consent is also required for the use of the data for further application procedures or before forwarding the application to other Group companies.

- In an existing employment relationship, data processing must always relate to the purpose of the employment contract if none of the following legal justifications for consent to data processing applies.

- If further information about the applicant must be collected from a third party during the initiation of the employment relationship or in the existing employment relationship, the respective national legal requirements must be taken into account. In cases of doubt, consent must be obtained from the data subject.

- For the processing of personal data in the context of the employment relationship, which are not originally used for the fulfilment of the employment contract, a legal legitimation must exist in each case. This may be legal requirements, collective agreements with employee representatives, an employee's consent or the legitimate interests of the company.

6.2.2 Collective Agreements on Data Processing

- If a data processing activity exceeds the purposes of fulfilling a contract, it may be permissible if authorised through a collective agreement. Collective agreements are wage agreements or agreements between employers and employee representatives within the scope of applicable labour law. These agreements must cover the specific purpose of the intended data processing activity and must be drawn up within the parameters of national data protection legislation.

6.2.3 Consent to Data Processing

- Employee data may be processed on the basis of the consent of the data subject. Declarations of consent must be submitted voluntarily. Voluntary status may be granted in particular if a legal or economic advantage is obtained for the person employed or if the employer and the person employed pursue the same interests. Involuntary consent is void. For the purpose of documentation, the declaration of consent must always be obtained in writing or electronically. If, in exceptional circumstances, this is not possible, consent may be given verbally. In any case, its granting must be properly documented. In the case of informed voluntary disclosure of data by the data subject, consent may be deemed to have been given if no explicit consent is required by national law. Before giving consent, the data subject must be informed in accordance with 5.3 of this Data Protection Guideline.

6.2.4 Data Processing Pursuant to Legitimate Interest

- Personal employee data may also be processed if this is necessary for the realisation of a legitimate interest of the GMC-I Group. Legitimate interests are usually of legal nature (e.g., the assertion, exercise or defence of legal claims) or commercial nature (e.g., proof of qualification).

- Personal data must not be processed on the basis of a legitimate interest if, in individual cases, there is evidence that the employee‘s interests worthy of protection have precedence over the interest in the processing. The existence of any interest worthy of protection shall be examined for each processing.

- Control measures that require processing of employee data may be taken only if there is a legal obligation to do so or there is a legitimate reason. Even if there is a justified reason, the proportionality of the control measure must be assessed. The legitimate interests of the company in performing the control measure (e.g., compliance with legal provisions and internal company rules) must be weighed against any interest worthy of protection that the employee affected by the measure may have in its exclusion and cannot be performed unless appropriate. The legitimate interest of the company and any interests of the employee worthy of protection must be identified and documented before any measure is taken. In addition, other requirements that may exist under national law (e.g., co-determination rights of employee representatives and information rights of data subjects) must be taken into account.

6.2.5 Processing of Sensitive Data

- Sensitive personal data may be processed only under certain conditions. Sensitive data means data concerning racial and ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or the health or sexual life of the data subject. Under national law, further data categories may be classified as sensitive or the data categories may have different contents. In addition, data relating to criminal offences may often only be processed under special conditions laid down by national law.

- The processing must be expressly permitted or prescribed under national law. The employee can voluntarily also give his or her express consent to the processing.

- If the processing of sensitive data is planned, the data protection officer must be informed in advance.

6.2.6 Automated Decisions

- If personal data are processed automatically as part of the employment relationship, and specific personal details are evaluated (e.g., as part of personnel selection or the evaluation of skill profiles), such automated processing must not be the sole basis for decisions that would have negative consequences or considerable impairments for the employees concerned. In order to avoid wrong decisions, automated procedures must ensure that the content of the facts is evaluated by a natural person and that this evaluation is the basis for the decision.

6.2.7 Telecommunications and Internet

- Telephone systems, e-mail addresses, intranet and internet as well as internal social networks are provided by the company for operational purposes only. They are tools and company resources. They may be used within the framework of the applicable legal provisions and the company‘s internal guidelines.

- In exceptional cases, limited use for private purposes may be permitted. However, this requires a corresponding written company guideline or a written approval in individual cases. In the case of permitted use for private purposes, the secrecy of telecommunications and the applicable national telecommunications law must be observed, to the extent that these apply.

- There will be no general monitoring of telephone and e-mail communication or of intranet and internet use. To defend against attacks on the IT infrastructure or on individual users, security measures may be implemented that block technically harmful contents or analyse the patterns of attacks. For security reasons, the use of telephone systems, e-mail addresses, the intranet and internet as well as internal social networks may be logged. Evaluations of such data relating to individuals may only be conducted in the event of a concrete, justified suspicion of a violation of laws or guidelines of the GMC-I Group or the respective company. Such checks may only be performed by investigating departments in compliance with the principle of proportionality. The respective national laws must be observed as well as the Group regulations in force for this purpose.

7 Transfer of Personal Data

- Any transfer of personal data to recipients outside or within the GMC-I Group is subject to the admissibility requirements for the processing of personal data in Section 6. The recipient of the data must be committed to use them only for the defined purposes.

- In the event that data are transferred to a recipient outside the GMC-I Group in a third country (outside of the European Economic Area), this recipient must guarantee to maintain a data protection level equivalent to this Data Protection Guideline. This does not apply if the transfer is based on a legal obligation. Such a legal obligation may arise from the law of the country in which the Group company which transfers the data has its registered office or the law of the country in which the Group company has its registered office recognises the objective of data transfer pursued by the legal obligation of a third country.

- In the case of data transfer from third parties to companies in the GMC-I Group, it must be ensured that the data may be used for the intended purposes.

- If personal data are transferred from a Group company with its registered office in the European Economic Area to a Group company with its registered office outside the European Economic Area (third country), the data-importing company is obliged to cooperate with the supervisory authority responsible for the data-exporting company in all inquiries and to observe the findings of the supervisory authority with regard to the transferred data. The same applies to data transfers by Group companies from other countries. If they are part of an international certification system for binding corporate rules on data protection, they must ensure the cooperation envisaged there with the relevant auditing bodies and authorities. Participation in such certification systems must be agreed with the management of the GMC-I Group.

- In the event that a data subject claims that this Data Protection Guideline has been breached by a data-importing Group company with its registered office in a third country, the data-exporting Group company with its registered office in the European Economic Area undertakes to support the data subject, whose data were collected in the European Economic Area, in establishing the facts of the matter and also asserting his/her rights in accordance with this Data Protection Guideline against the data-importing Group company. In addition, the data subject is also entitled to assert his or her rights against the Group company exporting the data. In the event of an alleged infringement, the data-exporting company must prove to the data subject that the data-importing Group company in a third country is not responsible for any infringement of this Data Protection Guideline if the data received are further processed.

8 Contract Processing

- Contract processing means that a service provider is commissioned to process personal data without being assigned responsibility for the associated business process. In such cases, an agreement on contract processing shall be concluded both with external service providers as well as between companies within the GMC-I Group. In this context, the contracting company retains full responsibility for the correct execution of data processing. The service provider may only process personal data in accordance with the instructions of the client. When placing the order, the following requirements must be observed; the department commissioning the order must ensure their implementation.

1. The service provider must be chosen based on its ability to cover the required technical and organisational protective measures.
2. The order must be placed in writing. The instructions on data processing and the responsibilities of the client and provider must be documented.
3. The contractual standards provided by the Group‘s data protection officer must be observed.
4. Before starting data processing, the client must verify compliance with the obligations of the provider. A provider can prove compliance with data security requirements in particular by presenting a suitable certification. Depending on the risk of data processing, the check may have to be repeated regularly during the term of the contract.
5. In the case of cross-border contract processing, the respective national requirements for the transfer of personal data abroad must be fulfilled. In particular, the processing of personal data from the European Economic Area may only be performed in a third country if the provider furnishes evidence of a level of data protection equivalent to that specified in this Data Protection Guideline. Suitable instruments may be:

a) Agreement on EU standard contract clauses for contract processing in third countries with the provider and any subcontractors.
b) Participation of the provider in a certification system accredited by the EU for the creation of a suitable data protection level.
c) Acknowledgement of binding corporate rules of the provider to create a suitable level of data protection by the responsible supervisory authorities for data protection.

9 Rights of the Data Subject

- Every data subject has the following rights. Their assertion must be processed immediately by the responsible department and must not lead to any disadvantages for the data subject.

- The data subject is entitled to request information as to which personal data about him/her have been stored and for what purpose. If the employment relationship provides for further view rights to documents of the employer (e.g., personnel file) in accordance with respective employment law, these shall remain unaffected.

- If personal data are transferred to third parties, information must be given about the identity of the recipient or the categories of recipients.
- If personal data are incorrect or incomplete, the data subject may request their correction or complementation.
- The data subject may object to the processing of his or her data for purposes of advertising or market/opinion research. The data must be blocked from these types of use.
- The data subject is entitled to request the deletion of his or her data if the legal basis for processing the data is missing or has ceased to exist. The same applies in the event that the purpose of data processing has lapsed due to expiry of time or for other reasons. Existing retention requirements and interests worthy of protection that conflict with deletion must be observed.
- The data subject has a fundamental right of objection to the processing of his or her data, which must be taken into account if his or her interest worthy of protection outweighs the interest in the processing due to a particular personal situation. This does not apply if a legal regulation requires the processing or legal retention periods make the storage of the personal data necessary.
- In addition, every data subject may assert the rights granted in Sections 5, 6, 7, 10 and 11 as a third-party beneficiary if a company that has undertaken to comply with this Data Protection Guideline fails to observe its provisions and thereby violates the data subject's rights.

10 Confidentiality of Processing

- Personal data are subject to data secrecy and confidentiality. Any unauthorised collection, processing, or use of such data by employees is prohibited. Any processing carried out by an employee without being entrusted with it within the scope of the performance of his or her duties and without being authorised accordingly is considered unauthorised. The "need-to-know" principle applies here: Employees may have access to personal data only if it is required for their particular task and to the extent necessary. This requires a careful allocation and separation of roles and responsibilities as well as their implementation and maintenance within the framework of authorisation concepts.
- Employees must not use personal data for their own private or commercial purposes, transfer or make them in any other way available to unauthorised persons.
- At the start of their employment relationship, superiors must inform their employees of their obligation to maintain data secrecy and confidentiality. This obligation shall remain in force even after employment has ended.

11 Security of Processing

- Personal data must be protected at all times against unauthorised access, unlawful processing or disclosure, as well as against loss, falsification or destruction. This applies regardless of whether the data are processed electronically or in paper form. Prior to the introduction of new data processing methods, in particular new IT systems, technical and organisational measures for the protection of personal data must be defined and implemented. These measures shall be based on the state of the art, implementation costs, the nature, scope, circumstances and purposes of processing and the varied likelihood and severity of the risks to rights and freedoms, the risks arising from processing and the protection requirements of the data (determined by the information classification process). The responsible department may consult in this regard the IT manager and the Group' s data protection officer. The technical and organisational measures for the protection of personal data are part of the Group-wide data protection management and must be continuously adapted to technical developments and organisational changes.

12 Data Protection Control

- Compliance with the data protection guidelines and the applicable data protection laws is regularly checked by means of data protection audits and other controls. The implementation of such controls is the responsibility of the Group's data protection officer or external auditors commissioned. The results of such data protection controls shall be communicated to the Group's data protection officer. The management of the GMC-I Group must be informed of material results within the framework of the respective reporting obligations. Upon request, the results of data protection controls shall be made available to the competent data protection supervisory authority. The competent data protection supervisory authority may also carry out its own inspections of compliance with the provisions of this Guideline within the limits of its powers under national law.

13 Data Protection Incidents

- Every employee must immediately report any violations of this Data Protection Guideline or other regulations for the protection of personal data (data protection incidents) to his or her respective superior, the IT manager and the Group's data protection officer. The manager responsible for the role or unit is obliged to inform the Group's data protection officer immediately of any data protection incidents.

  In the cases of
  - ➡ unauthorised disclosure of personal data to third parties,
  - ➡ unauthorised access by third parties to personal data, or
  - ➡ loss of personal data,

  the required company reports must be made immediately so that any reporting duties under national law regarding data protection incidents can be complied with.

14 Responsibilities

- The management boards of the Group companies are responsible for data processing in their areas of responsibility. They are thus obliged to ensure that the legal data protection requirements and those contained in this Data Protection Guideline are taken into account (e.g., national reporting requirements). It is a management task of the executives to ensure proper data processing in compliance with data protection through organisational, HR and technical measures. The implementation of these guidelines is the responsibility of the competent employees. In the event of any data protection controls by authorities, the management of GMC-Instruments GmbH must be informed immediately.

- The management boards of the Group companies may appoint a data protection officer for their company if this makes sense for the implementation of national data protection requirements.

- If there are criteria for the mandatory appointment of a data protection officer in accordance with national legal regulations or the GDPR, the managing director of the relevant Group company must appoint a data protection officer.

- If an individual company appoints a data protection officer, the management of GMC-Instruments GmbH must be informed immediately.

- The duties of the data protection officer are governed by the respective legal regulations.

Nuremberg, 01/01/2024
GMC-Instruments GmbH

Joachim Czabanski
Chairman of the Board

Matthias Wist
Member of the Board

GMC INSTRUMENTS

GMC-Instruments GmbH
Südwestpark 15 ■ 90449 Nürnberg ■ Germany
Phone: +49 911 252661-0 ■ Fax: +49 911 252661-881

www.gmc-instruments.com ■ info@gmc-i.com

Printed in Germany • Subject to change without notice • 2/01.24 • 3-336-015-03